Attorney Docket No. NC30561 Patent Application Papers of: Matthew Gast Express Mail Label No. EL620282941US

CLAIMS

What is claimed is:

1	1.	A method for providing network security, comprising the steps
2		of:
3		receiving a plurality of network protocol packets, wherein
4		a network protocol packet includes a network protocol header
5		and a plurality of network protocol data, and wherein the
6		network protocol data include a first cryptographic protocol
7		header and a first plurality of encrypted data;
8		determining a first plurality of cryptographic protocol rules
9		associated with the network protocol data;
10		establishing a cryptographic session, if required by said
11		first cryptographic rules;
12		applying the first plurality of cryptographic protocol rules
13		to the first encrypted data to obtain a first plurality of cleartext
14		data;
15		translating the first plurality of cleartext data into a second
16		plurality of cleartext data in accordance with at least one
17		translation rule; and
18		encrypting the second plurality of cleartext data in
19		accordance with at least one rule associated with a second
20		cryptographic protocol, resulting in a second plurality of
21		encrypted data.
1	2.	A system for providing network security, comprising:

Attorney Docket No. NC30561 Patent Application Papers of: Matthew Gast Express Mail Label No. EL620282941US

2		an input module for receiving a plurality of network protocol packets;
4 5		a translation module for translating a first plurality of data into a second plurality of data;
6		an output module; and
7 8		a cryptographic module responsive to the input module and the output module for performing cryptographic operations.
1	3.	A system for providing network security, comprising:
2		means for receiving a request to perform a cryptographic operation;
4 5		means for returning a response to the cryptographic operation request;
6 7		at least one module for performing said cryptographic operations.
1 2	4.	The method of claim 1, wherein the at least one translation rule is predetermined.
1 2	5.	The method of claim 1, wherein the at least one translation rule is determined dynamically.
1 2	6.	The method of claim 1, wherein the first cryptographic protocol is WTLS.
1 2	7.	The method of claim 1, wherein the first plurality of encrypted data is associated with WML.
1 2	8.	The method of claim 1, wherein second plurality of encrypted data is associated with HTML.

Attorney Docket No. NC30561
Patent Application Papers of: Matthew Gast Express Mail Label No. EL620282941US

1 2	9.	The method of claim 1, wherein the second cryptographic protocol is SSL over HTTP.
1 2	10.	The method of claim 1, wherein the first cryptographic protocol and the second cryptographic protocol are identical.
1 2 3 4	11.	The method of claim 1, wherein the first plurality of encrypted data and the second plurality of encrypted data conform to different revisions of a specification for the same cryptographic protocol.
1 2 3	12.	The system of claim 3, wherein at least one cryptographic module is a cryptographically strong pseudorandom number generator.
1 2	13.	The system of claim 3, wherein the cryptographic operations are performed using cryptographic acceleration hardware.
1 2 3	14.	The system of claim 13, wherein the cryptographic acceleration hardware includes a plurality of individual hardware acceleration units.
1 2	15.	The system of claim 14, wherein at least one individual hardware acceleration unit is dedicated to one function.
1 2 3	16.	The system of claim 13, wherein the cryptographic acceleration hardware is updateable by loading at least one cryptographically signed instruction.
1 2	17.	The system of claim 13, wherein the cryptographic acceleration hardware is tamper-resistant.
1 2	18.	The system of claim 13, wherein the cryptographic acceleration hardware is tamper-evident.